植基像素模數之可移除的可視浮水印技術

Removable Visible Watermarking Based on Pixel Modulus

楊政興
屏東教育大學資訊科學所
chyang@mail.npue.edu.tw

黃建銘
屏東教育大學資訊科學所
bm097119@mail.npue.edu.tw

孔芃勝
屏東教育大學資訊科學所
bm098114@mail.npue.edu.tw

鄭達懿
屏東教育大學資訊科學所
bm098119@mail.npue.edu.tw

摘要

數位浮水印 (Digital watermarking)是一項廣為被用來捍衛智慧財產權(Copyright)的一項技術，加入浮水印的目的，是希望在產權上加上一個類似商標的標記，當著作發生爭議時，可以藉由這個數位浮水印來判斷產權的合法所有者。本論文開發一套可逆的可視浮水印技術將黑白的二元浮水印影像嵌入到灰階影像，產生具可視浮水印的灰階影像。由於一般的嵌入和取出需要繁雜的計算，本文嘗試利用改變像素值的簡易方式來達成可視數位浮水印的嵌入，並且利用可逆的藏密學技術將浮水印資訊藏入，此額外藏入的浮水印資訊，可以用來恢復原始的影像。

關鍵詞—數位浮水印(Digital watermarking)、智慧財產權(Copyright)、藏密學(Steganography)。

一、前言

近年來，由於科技的進步以及網際網路的快速發展，許多數位資訊都在網際網路上傳送，資訊更快速且容易取得，然而傳送中的數位媒體資訊容易被竄改或是複製，也衍生出智慧財產權的保護及多媒體完整性的認證等問題，而數位浮水印是解決這個問題最直接的技術。數位浮水印，最主要的技術是將合法者的圖騰，加入到被保護的圖像中，從外觀來看可將數位浮水印技術分為兩大類：

1. 不可視浮水印(Invisible watermark)：不可視浮水印是不可以利用肉眼直接看見，且不容易破壞原始影像的外觀。
2. 可視浮水印(Visible watermark)：可視浮水印可以利用肉眼直接看見，其缺點是容易破壞原始影像的外觀，並且容易讓不法人士更改或抹去。

一般的數位浮水印可分成黑白浮水印(Binary watermark)與灰階浮水印(Gray level watermark) ，黑白浮水印是由 0、1 數值所組成的影像；而灰階浮水印是由 0~255 的數值所組成的影像。

藏密學(Steganography)是資訊隱藏技術中的一個議題，在數位化資訊與網際網路時代，藏密學技術的發展也起了很大的變化，許多將資訊隱藏於各種數位媒體的相關軟體已陸續被開發出來，各種傳播的影像都可能成為偽裝影像，加上影像、視訊等數位多媒體的資料量大，透過電腦處理，可以將人類感官系統所無法察覺的變化分析出來，藉由電腦的輔助，使用者可以輕易地將資訊大量隱藏於各種數位媒體之中，一般商業或個人的機密資訊，都可以利用這項技術來增加資訊的安全保護。

通常資訊隱藏在執行資訊嵌入前，藏密者會找出嵌入資料後，對原始影像破壞最小之下，進行機密資料的嵌入及取出等動作。一般而言，一個安全的藏密技術必須具備兩個要素，一是隱蔽性 (Imperceptibility) ，另一是藏量密容(Capacity)。但是大部分這兩大要素會呈現互相牽制的關係。當藏密容量越大時，則對影像的改變愈多，因而被察覺出來的可能性越高；反之藏密

容量限制越小量，則越不容易被察覺出來。

本研究利用可視浮水印的技術和黑白浮水印較小的資料量，對影像做浮水印的嵌入，受保護的影像上可以清楚的看見黑白浮水印的樣貌。嵌入的過程中沒有繁雜的轉換，直接利用像素值的改變來達成可視的效果，並且利用可逆的藏密學技術將浮水印資訊藏入，此額外藏入的浮水印資訊，可以用來恢復原始的影像。本論文其他部分如下，第二節為文獻探討，第三節介紹我們的可視浮水印技術，第四節為實驗結果，第五節提出結論及未來研究方向。

二、文獻探討

數位浮水印的作用是保護著作所有權，當受保護的影像遭遇攻擊時，當中的數位浮水印必須確保不被移除，以利所有權的判斷。其中，嵌入強韌的浮水印較能抵抗一般的攻擊；然而，強韌的浮水印在嵌入過程中對於原始影像的影響也越大。因此，追求浮水印的強韌性以及保持原始影像的品質這兩點，就成了研究數位浮水印的重要議題[3]。

現今數位浮水印的技術中，有許多是在分析數位浮水印的嵌入機制，探討如何減少對原始影像品質的影響，並且嵌入更多的、更強韌的浮水印資訊[3, 4]，在論文[4]中則提出一個利用JND(Just Noticeable Distortion)模式來計算影像特性，將數位浮水印以不同強度嵌入影像的機制，但其演算法在驗證時必須參考原始影像才能取回數位浮水印，在無法取得原始影像的情況下，此機制便無法發揮效用。

另有一種機制是不需對原始影像嵌入任何資料即可認證該影像的所有權[5, 6]。其方法是以影像特徵作為認證樣本，將其處理後予以記錄；在驗證時，只要影像的特徵仍然存在，與所儲存之資料作對比後即可證明其所有權。這種方式雖然對原始影像是無損的，但就因為這類機制並沒有對影像做任何嵌入修改的動作，因而即使該影像已通過驗證，其正當性仍略有不足。

在論文[1]中提到不同於一般直接將特定數位浮水印嵌入原始影像的浮水印嵌入機制，先透過結合影像特徵與特定浮水印以產生一私密認證樣本，再將此樣本嵌入欲保護的原始影像中，而嵌入時會依照影像內容特性調整其嵌入強度。驗證時，取回其中包含的私密認證樣本與影像的特徵並結合後，即可還原浮水印。

嵌入的方式：先將欲保護的原始影像以DWT 轉為頻率域係數，抽取出其特徵，並與打散的浮水印結合後，生成私密認證樣本，並將其嵌入原始影像後，再以 IDWT 轉換回含嵌入資訊的影像。

浮水印的取回：首先待驗證的影像經過二階的 DWT 轉換，從係數中抽取特徵與樣本，結合特徵與樣本以取回打散的浮水印，再將其還原後，與原始浮水印比較以驗證其所有權。

在論文[8]中，提出了可逆可視浮水印技術，一方面嵌入可視浮水印另一方面也嵌入不可視的浮水印資訊，為了滿足高容量以及良好的影像品質，採用的隱藏技術是基於數據壓縮。

論文[9]所提出的方法是將可視浮水印嵌入到原始影像內，再將浮水印資訊藏入未嵌入浮水印的區域，然而可利用這些資訊來恢復被攻擊影像中的浮水印。

在論文[10]中，提出了可逆式可視浮水印技術，可以完全恢復原始影像，首先將要嵌入浮水印區域的像素值縮小成$[\alpha,\ \alpha+127]$，其中α為原像素值的一半，再將浮水印嵌入，並利用密鑰調整透明度和強韌性，最後將差分影像壓縮並可逆式嵌入，做為恢復原始影像之用

論文[2]中，提出直方圖式可逆資訊隱藏技術，採用交錯式預測編碼方法，提高直方圖中高點的高度，以增加資訊的嵌入量。論文中提出的預測編碼方法，利用偶數行來預測奇數行，然後再利用奇數行來預測偶數行，將一張影像中所有的像素值都做預測編碼，充分利用每一個像素

值，並且藏入機密訊息後的偽裝影像，每個像素值的改變量均小於或等於 1，保持原始影像和偽裝影像的相似度。

三、我們的可視浮水印的方法

本研究提出利用黑白的二元影像嵌入到灰階影像，改變像素值的方式來達成數位浮水印的嵌入，並利用額外嵌入浮水印資訊的方式來達到可恢復原始影像的目的。以下分別對數位浮水印的嵌入及移除程序，加以介紹。

3.1 數位浮水印的藏入程序

首先對原始影像和數位浮水印作定義：

$$X=\{x(i,j)\mid 0\leqq i<M,\ 0\leqq j<M\}$$

$$W=\{w(i,j)\mid 0\leqq i<N,\ 0\leqq j<N\}$$

X 代表原始影像，W 代表數位浮水印，i 代表影像的 x 座標，j 代表影像的 y 座標，原始影像大小為 $M \times M$，數位浮水印的大小為 $N \times N$，原始影像為灰階影像每個像素值範圍為 0~255，數位浮水印採用二元影像每個像素值為 0 或 1。圖 1 顯示嵌入浮水印的流程圖，先確定原始影像 X 要嵌入浮水印的區域，然後將浮水印以可視的方式嵌入，產生影像 X'，最後再將浮水印等資訊以可逆的不可視方式來嵌入，產生影像 X''。詳細的浮水印嵌入步驟如下：

輸入：原始影像 X、數位浮水印 W、嵌入區域、亂數種子 K、距離參數 D。

步驟 1：讀取數位浮水印的像素值 $w(i, j)$，順序為由左而右，由上到下。另外，依指定的嵌入區域，由左而右，由上而下讀取原始影像 X 對應的像素值 $x(i, j)$，當讀取的浮水印 $w(i, j)$為 0 時，保留原始像素 x(i,j)值，即 $x'(i, j) = x(i, j)$；當讀取的浮水印 $w(i, j)$為 1 時，做下列運算：

$$x'(\mathrm{i,j}) = x(i, j) + R(i, j) \pmod{256} \quad (1)$$

，其中 $x'(i, j)$為更改過後的像數值，R 為利用亂數種子 K 產生的介於 D 到 $-D$ (mod 256)之間的正整數。

步驟 2：將數位浮水印 W 和嵌入區域等資訊，利用可逆藏密學技術藏入於影像 X'，最後產生影像 X''。

步驟 3：輸出嵌入後的影像 X''。

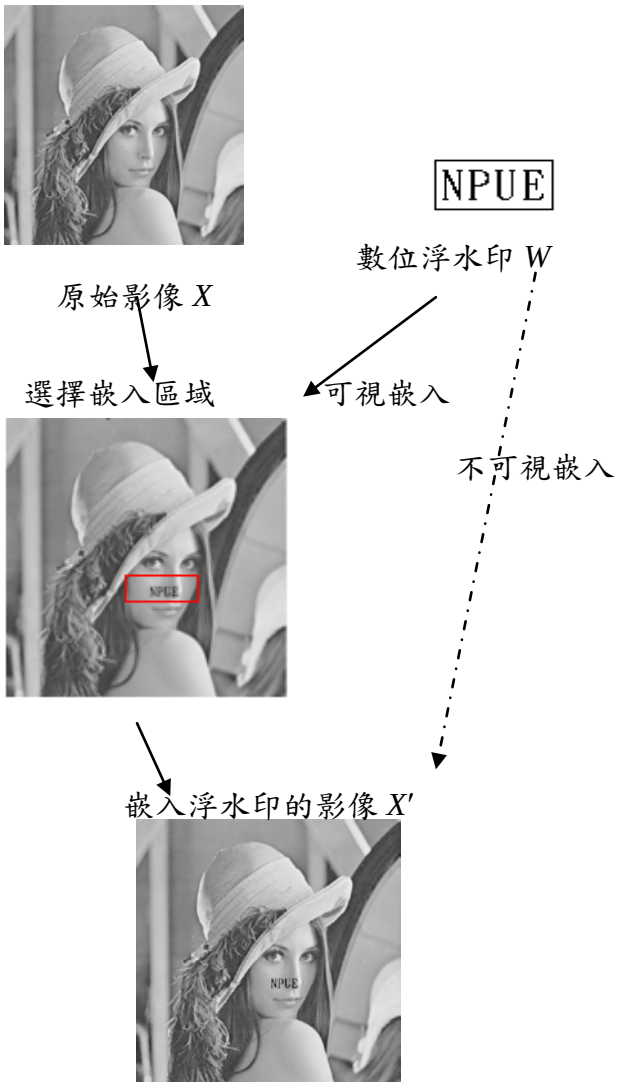


圖 1 數位浮水印嵌入流程

3.2 數位浮水印的取出和移除程序

圖 2 顯示取出和移除浮水印的流程圖，從嵌入浮水印和資訊的影像 X''，取出浮水印和嵌入區域等資訊，並回復成影像 X'，接著，移除影像 X'上的可視浮水印，回復成原始影像 X。詳細的浮水印取出和移除步驟如下：

輸入：已嵌入浮水印和資訊的影像 X''、亂數種

子 K、距離參數 D。

步驟 1：利用可逆方式，從影像 X''中取出藏入的數位浮水印 W和嵌入區域等資訊，並回復成影像 X'。

步驟 2：讀取數位浮水印 W的像素值，順序為由左而右，由上到下。另外，依嵌入區域之資訊，由左而右，由上而下讀取影像 X'對應的像素值 $x'(i, j)$。當讀取的浮水印 $w(i, j)$為 0 時，保留原像 素值，即 $x(i, j) = x'(i, j)$；當讀取的浮水印 $w(i, j)$為 1 時，做下列運算：

$$x(i, j) = x'(i, j) - R(i, j) \pmod{256} \quad (2)$$

步驟 3：輸出回復後的影像 X。

嵌入浮水印和資訊的影像 X''

移除嵌入的不可視資訊

取出浮水印和
嵌入區域等資訊

回復的影像 X'

浮水印

原始影像 X

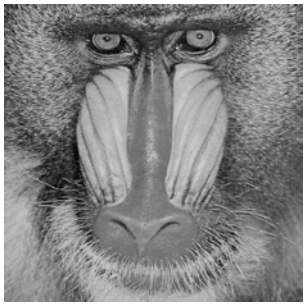
圖 2 數位浮水印取出和移除流程

四、實驗結果

本節針對我們提出的方法加以實驗分析。圖 3 為實驗用的二元浮水印，大小為 300 × 150。圖 4 為受保護的 4 張灰階影像，大小為 512 × 512。

圖 3 二元浮水印

(a)Lean



(b)Baboon

(c)Girl

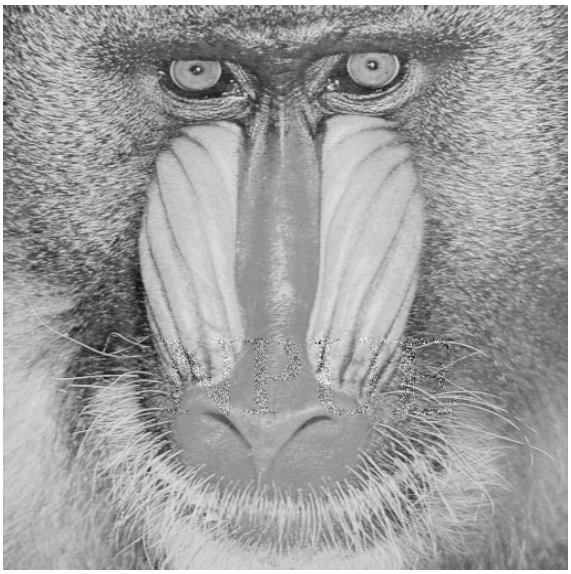
(d) Peppers

圖 4　512 × 512 灰階影像

圖 5 為利用可視方式嵌入浮水印，並且利用交錯式預測法之可逆的不可視方式嵌入浮水印資訊的結果[2]，其中距離參數 $D = 64$，即公式(1)

的 R 值範圍介於-64~64 之間。由結果可以看出，影像上清楚顯示浮水印標記。表 1，表 2 和表 3，利用 PSNR(Peak Signal to Noise Ratios)值來評估影像值嵌入 PSNR(Peak Signal to Noise Ratios)值來評估影像 X，X'和 X''間的相似性。表 1 為藏入不可視浮水印的影像 X'，對應於原始影像 X 的 PSNR 值。表 2 為藏入不可視浮水印資訊的影像 X''，對應於影像 X'之 PSNR 值。表 3 為藏入可視和不可視浮水印的影像 X''，對應於原始影像 X 之 PSNR 值。

(a)Lena



(b)Baboon

(c)Girl

(d)Peppers

圖 5　已嵌入浮水印的影像

表 1 影像 X'對應於原始影像 X 的 PSNR 值

	Lean	Baboon	Girl	Peppers
PSNR	29.137	32.277	32.340	30.856

表 2 影像 X''對應於影像 X'之 PSNR 值

	Lena	Baboon	Girl	Peppers
PSNR	48.654	48.127	48.628	48.247

表 3　有藏入可視浮水印、不可視浮水印 X”與原始影像 X 之 PSNR 值

	Lena	Baboon	Girl	Peppers
PSNR	29.017	27.554	27.887	27.046

距離參數 D 不同會產生不同的影像，圖 6 為測試結果。

(a) D=96

(b) D=32

圖 6　使用不同的 D 值所產生的影像

在嵌入浮水印區域,任意假定 D 值在不知道 K 值的情況下，測試 D=64 的影像是否能將浮水印消除。圖 7 為測試的結果。因不知道 K 值，而任意假定 D 值是無法消除浮水印。

（a）D=40

(b) D=64

圖 7　任意假定 D 值在不知道 K 值所產生的影像

五、結論

本研究利用可視浮水印的技術和黑白浮水印較小的資料量，對影像做浮水印的嵌入，受保護的影像上可以清楚的看見黑白浮水印的樣貌，研究中嵌入的 D 值越大對原始影像所造成的影響：

1. 嵌入後的影像之 PSNR 值越小，但浮水印的效果會越清楚。
2. 浮水印效果比較缺乏透明性。
3. 在高頻區域可以明確的看出可視浮水印。
4. 會將原始影像的特徵掩蓋。
5. 安全性越高(產生的亂數範圍較大，要恢復越困難) 。

此外利用可逆的資訊隱藏技術，將浮水印資訊藏入，其對應的 PSNR 值在 48 以上，所以不會影響具有可視浮水印的影像之品質，這些資訊可以進一步取出來，用於移除可視浮水印。實驗結果顯示，我們的技術可以清楚顯示浮水印，並且可以將浮水印移除。

致謝

本研究接受國科會之計畫編號：NSC 98-2221-E-153-001 的部分經費補助。

參考文獻

1. 謝尚琳, 葉中平, 蔡依儒 黃彬原, “一個嵌入強度與影像內容相關的浮水印機制,” in 2008 數位科技與創新管理研討會, 2008。
2. 楊政興, 蔡孟璇, 黃建銘, 吳敏豪, “植基於交錯式預測法之可逆資訊隱藏技術,” in TANET 2008台灣網際網路研討會, 義守大學, pp. 127-132, October 20-22, 2008。
3. Guzman, V.V.F., Miyatake, M.N., and Meana, H.M.H., "Analysis of a wavelet-based watermarking algorithm," IEEE International Conference on Electronics, Communications and Computers, pp.283-287, Feb. 2004.
4. Fan Zhang and Honghin Zhang, "Digital watermarking capacity research," IEEE International Conference on Communications, Circuits and Systems**,** Vol.2, pp.796-799, June 2004.
5. Chuan-Yu Chang and Sheng-Jyun Su, "Apply the counter propagation neural network to digital image watermarking," IEEE International Workshop on Cellular Neural Networks and Their Applications, pp.110-113, May 2005.
6. Der-Chyuan Lou, Jieh-Ming Shieh, and Hao-Kuan Tso, "Copyright orotection schemebased on chaos and secret sharing techniques," SPIE Optical Engineering, Vol. 44, Issue 11, pp.117004-117011, Nov 2005.
7. Y. J. Hu, S. Kwong, and J. Huang, “An algorithm for removable visible watermarking,” IEEE Trans. Circuits Syst.

Video Technol., vol. 16, no.1, pp. 129–133, Jan. 2006.

8. Y. Hu, and B. Jeon, “Reversible visible watermarking and lossless recovery of original images,” IEEE Transactions on Circuits andSystems for Video Technology, vol.16, No.11. pp. 1423-1429, Nov 2006.
9. S.-C. Shie and S. D. Lin” Improving robustness of visible image watermarks”Imaging Science Journal, The, Vol. 56, No. 1. pp. 23-28, February 2008.
10. Han-Min Tsai, Long-Wen Chang, “A high secure reversible visible watermarking scheme” IEEE International Conference on Multimedia and Expo, Pages 2106-2109, 2007.